WEST Search History

Hide Items | Restore | Clear | Cancel

DATE: Thursday, March 24, 2005

Hide?	Set Name	Query	Hit Count
		DB=PGPB,USPT,USOC,EPAB,JPAB,DWPI,TDBD; PLUR=YES; OP=OR	
☐	L11	L9 same "input block"	6
☐	L10	L9 same "keyed function"	0
☐	L9	"message authentication code" same "input block"	6
☐	L8	L7 same "hash"	14
☐	L7	"message authentication code" same "compression function"	15
☐	L6	705/67.ccls.	313
☐	L5	380/270.ccls.	505
☐	L4	380/274.ccls.	125
☐	L3	705/67.ccls.	313
☐	L2	713/156.ccls.	456
☐	L1	patel.in. and sarver.in.	1

END OF SEARCH HISTORY

Web Results 1 - 10 of about 9,730 for **authentication iteration hash encryption key message authentication**

RFC2898
... iterationCount specifies the **iteration** count. ... M. and R. Canetti, "HMAC: Keyed-**Hashing** for **Message Authentication**", RFC 2104 ... FIPS PUB 180-1: Secure **Hash** Standard ...
www.scit.wlv.ac.uk/rfc/rfc28xx/RFC2898.html - 68k - Mar 23, 2005 - Cached - Similar pages

SSL/TLS Terms and Acronyms (Including Some General Cryptography ...
... block of random data used as the initial chaining value for the first **iteration** of Cypher ... MAC **Message Authentication Code**. A **key**-dependent one-way **hash** function ...
www.technoids.org/tlsglossary.html - 27k - Cached - Similar pages

About SSL/TLS
... The **authentication** is done by concatenating a secret **key** to ... the **hash** function before passing it to the second **iteration**. ... As a **hash** function, SSL can use MD5 or ...
www.cs.bham.ac.uk/~mdr/teaching/ modules03/security/students/SS8a/SSL.TLS.html - 25k - Mar 24, 2005 - Cached - Similar pages

[PDF] A comparison of FIPS PUB 113 and HMAC
File Format: PDF/Adobe Acrobat - View as HTML
... of the bits re- sulting from the last **iteration**, are used as the Data **Authentication Code** (DAC ... It uses existing **hashing** algorithms with no **key** input, into ...
www.stud.ntnu.no/~havarmor/fag/art/46.pdf - Similar pages

[PPT] Security
File Format: Microsoft Powerpoint 97 - View as HTML
... **Iteration** block. ... **Message Authentication**: means a receiver has to be sure of the sender's identity. ... To create a digest a "**hash** function" is used. ...
www.cs.geneseo.edu/~fritz/ cs104-04S/Lectures/cs104-security.ppt - Similar pages

[PDF] An abridged version of this paper appears in Advances in ...
File Format: PDF/Adobe Acrobat - View as HTML
... as the ideality" of the underlying **hash** functions ... function is pseudo-random then so is its **iteration**. ... as the mandatory to implement **authentication** transform for ...
www.cs.ucsd.edu/users/mihir/papers/kmd5.pdf - Similar pages

CFRG Working Group T. Krovetz, Editor INTERNET-DRAFT CSU ...
... iters * 4) // // For each **iteration**, extract **key** ... end for // // Inner-product **hash**, extract last ... a specification of a **message authentication code**, this entire ...
www.ietf.org/internet-drafts/draft-krovetz-umac-02.txt - 43k - Cached - Similar pages

[PDF] 5 Computer Networks Communications Architecture and Protocols
File Format: PDF/Adobe Acrobat - View as HTML
... from one **iteration** as input to next DES **iteration** Use different ... Generate **authentication code** based on shared **key** and **message** Common **key** ... One Way **Hash** Function ...
duck.cs.und.ac.za/~tanja/Webpage/Networks/part13.pdf - Similar pages

United States Patent Application: 0030203756
... the output of a one-way **hash** function, any ... knowledge proof algorithm can be adapted to perform **authentication**. ... algorithm will contain for each **iteration**: 1) a ...
appft1.uspto.gov/.../%22shuffle+master%22&RS=IN/ %22jackson,+mark%22+AND+AN/%22shuffle+master%22 -

101k - Mar 24, 2005 - Cached - Similar pages

[PDF] Microsoft PowerPoint - ho2005.ppt
File Format: PDF/Adobe Acrobat - View as HTML
... message per **iteration** – x t-1 possibly padded ... length of the unpadded **message** • MD-strengthening – collisions in the **hash** function ⇒ collisions in the ...
www.isg.rhul.ac.uk/msc/teaching/opt8/week6-2005.pdf - Similar pages

Gooooooooooogle ▶
Result Page: 1 2 3 4 5 6 7 8 9 10 **Next**

authentication iteration hash encrypt Search

Search within results | Language Tools | Search Tips | Dissatisfied? Help us improve

Google Home - Advertising Programs - Business Solutions - About Google